Cyber Guru

Browser Defender

ANALYSE WEB EN TEMPS RÉEL POUR QUE LES ÉQUIPES AIENT DE BONS RÉFLEXES

Les formations de sensibilisation permettent d'ancrer des comportements sécurisés, mais elles ne sont pas suffisantes dans le paysage actuel des menaces, en constante évolution.

Vos employés accèdent quotidiennement au web pour effectuer des recherches, collaborer et utiliser des outils en ligne. En cliquant sur des liens, en téléchargeant des fichiers, en installant des extensions ou en se connectant à des applications tierces, ils prennent des décisions en matière de sécurité qui ont un impact sur votre organisation.

Pour renforcer les bons réflexes, limiter les erreurs humaines et réduire les cyber-risques, il est essentiel de les accompagner en continu.

Browser Defender complète les navigateurs standards en détectant en temps réel les comportements à risque et en appliquant des règles de sécurité sur les fichiers téléchargés et les extensions utilisées. Il guide les utilisateurs à chaque point de friction, leur permettant de prendre des décisions plus sûres en ligne.

Résultat : une posture de cybersécurité plus réactive et mieux ancrée dans votre organisation.

Des **garde-fous** en **temps réel face** à des **risques bien réels**

Sensibilisation intégrée au navigateur et alimentée par l'IA

Module complémentaire pour Firefox, Chrome, Edge et d'autres navigateurs Chromium, offrant une sensibilisation à la sécurité en temps réel sans perturber les flux de travail ni remplacer les navigateurs.

Alertes proactives en cas de phishing et de sites à risque

Prévient les utilisateurs avant qu'ils n'accèdent à des sites suspects ou ne saisissent leurs identifiants, les incitant à faire une pause et à agir en conscience, quel que soit leur niveau de sensibilisation.

Détection de la réutilisation d'identifiants professionnels

Alerte les équipes de sécurité en cas de réutilisation d'identifiants sur des sites tiers, ce qui permet de réagir plus rapidement et de réduire le risque de compromission des comptes.

Contrôle granulaire des téléchargements

Gère les téléchargements de fichiers en fonction du rôle de l'utilisateur et des politiques de votre organisation pour réduire les risques de phishing et de logiciels malveillants.

Gouvernance des extensions de navigateur

Bloque les extensions à risque ou non autorisées, limitant ainsi l'exposition aux menaces tout en respectant les règles internes.

Déploiement simple et centralisé

Installation à l'échelle de l'organisation via Microsoft Intune, GPO ou les stores de navigateurs, garantissant une adoption rapide.

Outils de pilotage conviviaux

Autorisez ou bloquez des domaines, fichiers ou extensions à grande échelle. Les signalements des utilisateurs enrichissent la surface de détection et renforcent la sécurité.

Suivre les progrès et mesure de l'impact

Tableaux de bord et rapports détaillés pour une visibilité claire et des actions ciblées.

Fonctionnalités de la connaissance du web en temps réel

SÉCURITÉ DE NAVIGATION

- Navigation sécurisée
- Détection de la réutilisation d'identifiants
- Contrôle des téléchargements et extensions
- Gouvernance des extensions

EXPÉRIENCE UTILISATEUR INTUITIVE ET EFFICACE

- Alertes instantanées ou blocage (configurable par l'administrateur)
- Support multilingue
- Analyse IA de haute précision
- Impact immédiat, quel que soit le niveau de sensibilisation

SOLUTION DE NIVEAU ENTREPRISE

- Plate-forme SaaS
- Add-on pour les navigateurs standards
- Déploiement centralisé simplifié
- Outils d'administration conviviaux
- Tableaux de bord et rapports intégrés